

日 本 国 特 許 庁
JAPAN PATENT OFFICE

14.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 1 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 4 1 6 1 8 8
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 4 1 6 1 8 8]

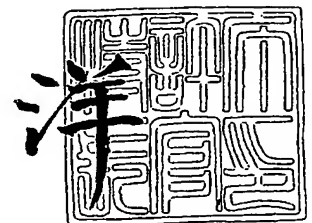
出 願 人 松 下 電 器 産 業 株 式 会 社
Applicant(s):



2 0 0 5 年 1 月 2 0 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2032750139
【提出日】 平成15年12月15日
【あて先】 特許庁長官殿
【国際特許分類】 H04L 9/00
G06K 19/00
G06K 17/00

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 中野 育恵

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 生駒 達郎

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 横田 博史

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】 辻 敦宏

【発明者】
【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 株式会社松下ソフトリサーチ内
【氏名】 山内 実

【特許出願人】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社

【代理人】
【識別番号】 100097445
【弁理士】
【氏名又は名称】 岩橋 文雄

【選任した代理人】
【識別番号】 100103355
【弁理士】
【氏名又は名称】 坂口 智康

【選任した代理人】
【識別番号】 100109667
【弁理士】
【氏名又は名称】 内藤 浩樹

【手数料の表示】
【予納台帳番号】 011305
【納付金額】 21,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

ネットワークを介して接続された複数の通信機器と、
前記ネットワークに接続されない秘密情報生成装置を備えたシステムにおける
機器間認証の初期設定方法であって、
前記秘密情報生成装置を用いて秘密情報を生成し、
生成した秘密情報をネットワークを介さずに
前記複数の通信機器に設定することを特徴とする、
秘密情報初期設定方法。

【請求項 2】

ネットワークを介して接続された複数の通信機器と、
前記ネットワークに接続されない秘密情報生成装置を備えたシステムにおいて、
前記秘密情報生成装置を用いて秘密情報を生成し、
生成した秘密情報をネットワークを介さずに前記複数の通信機器に設定し、
前記複数の通信機器に設定されている秘密情報の少なくとも一部が一致することを
ネットワークを介して確認することで認証を行うことを特徴とする、
認証システム。

【請求項 3】

第 1 の通信機器とネットワークを介して接続された第 2 の通信機器と、
前記第 1 の通信機器と前記第 2 の通信機器が認証のために用いる秘密情報を生成する秘
密情報生成装置を備えたシステムにおいて、
前記第 1 の通信機器が、前記第 2 の通信機器を認証する認証方法であって、
前記第 1 の通信機器と前記第 2 の通信機器間の認証の関係を初期設定する際に
前記秘密情報生成装置において秘密情報を生成する生成工程と、
生成した秘密情報を秘密情報生成装置内に記憶する記憶工程と、
前記第 1 の通信機器と前記第 2 の通信機器に
秘密情報生成装置内に記憶された秘密情報を設定する設定工程とを備え、
さらに前記第 1 の通信機器が、前記第 2 の通信機器を認証する際に
前記第 1 の通信機器は、前記第 2 の通信機器に設定されている秘密情報と
前記第 1 の通信機器に設定されている秘密情報の少なくとも一部が一致することを
ネットワークを介して確認する認証工程、を有することを特徴とする認証方法。

【請求項 4】

前記設定工程が実施されれば前記秘密情報生成装置内に記憶された秘密情報を
消去する秘密情報自動消去工程、をさらに有することを特徴とする、
請求項 3 に記載の認証方法。

【請求項 5】

操作者が指示するならば前記第 1 の通信機器と前記第 2 の通信機器に設定された秘密情報
を
消去する機器初期化工程、をさらに有することを特徴とする、
請求項 3 または請求項 4 に記載の認証方法。

【請求項 6】

操作者が指示するならば前記秘密情報生成装置に記憶された秘密情報を
消去する装置初期化工程、をさらに有することを特徴とする、
請求項 3 ないし請求項 5 のいずれか 1 項に記載の認証方法。

【請求項 7】

第 1 の通信機器とネットワークを介して接続された第 2 の通信機器と、
前記第 1 の通信機器と前記第 2 の通信機器が認証のために用いる秘密情報を生成する
秘密情報生成装置を備えたシステムにおいて、
前記第 1 の通信機器が、前記第 2 の通信機器を認証する認証方法であって、
前記第 1 の通信機器と前記第 2 の通信機器間の認証の関係を初期設定する際に

前記秘密情報生成装置において秘密情報を生成し、
生成した秘密情報を秘密情報生成装置内に記憶し、
前記第 1 の通信機器と前記第 2 の通信機器に秘密情報生成装置内に記憶された秘密情報を設定し、
前記第 1 の通信機器が、前記第 2 の通信機器を認証する際に
前記第 1 の通信機器は、前記第 2 の通信機器に設定されている秘密情報と
前記第 1 の通信機器に設定されている秘密情報の少なくとも一部が一致することを
ネットワークを介して確認する認証方法。

【請求項 8】

前記秘密情報は擬似乱数であることを特徴とする、
請求項 3 ないし請求項 7 のいずれか 1 項に記載の認証方法。

【請求項 9】

前記秘密情報は、
操作者には、理解できる形態において表示もしくは出力されないことを特徴とする、
請求項 3 ないし請求項 8 のいずれか 1 項に記載の認証方法。

【請求項 10】

ネットワークに接続された通信機器であって、
前記ネットワークに接続された所定の通信機器との認証の関係を初期設定する際に
外部から転送される秘密情報を取り込む第 1 の転送手段と、
取り込んだ秘密情報を記憶する第 1 の記憶手段と、を備え、
さらにネットワークを介してメッセージを送受信する通信手段と、
前記秘密情報から認証情報を生成する認証情報生成手段と、
前記所定の通信機器が前記ネットワークと前記通信手段を介して
提示する認証情報と生成した認証情報とが一致することを確認する検証手段と、
を有することを特徴とする通信機器。

【請求項 11】

操作者が前記通信機器の秘密情報の初期化指示を入力する第 1 の初期化指示手段と、
前記第 1 の初期化指示手段に入力された指示を受けて
前記第 1 の記憶手段に記憶された秘密情報を消去する第 1 の消去手段、をさらに有する
ことを特徴とする
請求項 10 に記載の通信機器。

【請求項 12】

前記第 1 の記憶手段が秘密情報を記憶しているかいないかを表示する第 1 の表示手段、を
さらに有することを特徴とする
請求項 10 または請求項 11 に記載の通信機器。

【請求項 13】

前記検証手段が認証情報の一致確認に成功したか否かを表示する第 2 の表示手段、をさら
に有することを特徴とする
請求項 11 または請求項 12 に記載の通信機器。

【請求項 14】

前記秘密情報は、
操作者には理解できる形態において表示もしくは出力されないことを特徴とする、
請求項 11 ないし請求項 13 のいずれかに記載の通信機器。

【請求項 15】

第 1 の通信機器と第 2 の通信機器間の認証の関係を初期設定する際に
操作者が秘密情報の生成指示を入力する生成指示手段と、
前記生成指示手段に入力された指示を受けて
秘密情報を生成する秘密情報生成手段と、
生成した秘密情報を記憶する第 2 の記憶手段と、
秘密情報を外部に転送する第 2 の転送手段と、

秘密情報を規定回数転送すると

前記第2の記憶手段に記憶された秘密情報を消去する第2の消去手段と、
を有することを特徴とする秘密情報生成装置。

【請求項16】

操作者が前記秘密情報の初期化指示を入力する第2の初期化指示手段をさらに備え、
前記第2の消去手段は、さらに前記第2の初期化指示手段に入力された指示を受けて
前記第2の記憶手段に記憶された秘密情報を消去することを特徴とする、
請求項15に記載の秘密情報生成装置。

【請求項17】

前記第2の記憶手段が秘密情報を記憶しているかいないかを表示する
第3の表示手段、をさらに有することを特徴とする、
請求項15または請求項16に記載の秘密情報生成装置。

【請求項18】

前記秘密情報は、
擬似乱数であることを特徴とする、
請求項15ないし請求項17のいずれか1項に記載の秘密情報生成装置。

【請求項19】

前記秘密情報は、
操作者には理解できる形態において表示もしくは出力されないことを特徴とする、
請求項15ないし請求項18のいずれか1項に記載の秘密情報生成装置。

【請求項20】

前記秘密情報生成装置は、
可搬型の装置であることを特徴とする、
請求項15ないし請求項19のいずれか1項に記載の秘密情報生成装置。

【書類名】明細書

【発明の名称】通信機器の認証システム、認証方法、通信機器および秘密情報生成装置

【技術分野】

【0001】

本発明は、ネットワークに接続する機器の認証方法に関し、特に、機器の演算処理負荷が少なく、簡単でかつ安全な認証方法に関する。

【背景技術】

【0002】

近年、インターネットを中心としたIP（インターネットプロトコル）ネットワークが急速に拡大し、PCの他、AV機器や監視カメラ、IP電話等のさまざまな家電機器がIPネットワークに接続する傾向にある。また、家庭内にIPネットワークを張りめぐらし、家電機器間での通信サービスを提供する機運も高まっている。しかし、一般的に、ネットワークを介して家電機器間で通信を行うとき、なりすましや外部からの侵入といった脅威に対処しなくてはならない。

【0003】

これらの脅威から情報を保護するためのセキュリティ技術の1つとして、通信相手の機器が正当な機器であることを確認する機器認証が用いられている。

【0004】

従来の通信機器間の認証方法としては、公開鍵暗号方式とデジタル署名を組み合わせた方式や、共通鍵を用いたチャレンジ・アンド・レスポンス方式などがある。

【0005】

例えば、証明書の交換に先だって交換される、通信相手の装置が発生した乱数から算出された情報に対して、認証時にデジタル署名を行うというものがあった。（例えば、特許文献1参照）。図9は、前記特許文献1に記載された従来の機器の認証方法を示すものである。

【0006】

図9において、STA1で乱数A1を生成し、Diffie-Hellman鍵配送アルゴリズムにより $GA1 \bmod P$ をSTA2へ送り、STA2ではA2を生成し、 $GA2 \bmod P$ をSTA1へ送り、STA1、STA2で共有鍵 $GA1 \cdot A2 \bmod P$ を得る。STA2はSTA2の公開鍵PK2の認証局による証明書とその秘密鍵K2による $GA1 \bmod P$ に対する署名C2をSTA1へ送り、STA1はその公開鍵PK1の証明書とその署名用鍵K1による $GGA2 \bmod P$ に対する署名C1をSTA2へ送る。各STA1、STA2では受信情報から、その公開鍵の正当性を確認し、かつその公開鍵で署名の検証を行っていた。

【0007】

また、ネットワークに接続された家電端末に認証タグを用いて必要な情報を取得させて鍵管理装置と認証を行い、認証成功に伴い鍵管理装置から家庭内の通信に使用される共通暗号鍵を受けとり、家庭内のネットワークに接続された家電端末同士で暗号化通信を行うものがあった（例えば、特許文献2参照）。図10は、前記特許文献2に記載された従来の機器の認証方法を示すものである。

【0008】

図10において、家電端末101と鍵管理装置103がネットワーク接続手段106を介して家庭内のネットワーク105に接続されており、認証タグ102を家電端末101に挿入する事で、鍵管理装置103と認証を行い、家庭内のネットワーク105に接続された他の家電端末101と通信を行うための共通暗号鍵を取得する事で、ネットワーク接続手段106を介してネットワーク105に接続された家電端末同士で暗号化通信を行っていた。

【特許文献1】特許第3253060号公報（第8頁、図1）

【特許文献2】特開2003-87238号公報（第9頁、図1）

【発明の開示】

【発明が解決しようとする課題】**【0009】**

しかしながら、公開鍵暗号方式を用いた方式は、第三者機関による公開鍵証明を行い、証明書を発行する機関が必要となるため扱いが複雑であり、また、一般的に機器の公開鍵暗復号演算ならびに電子署名演算の処理負担が高く、CPUやメモリ等リソースが乏しい機器には適していない。

【0010】

一方、共通鍵を用いた方式は、共通鍵を共有する過程で、認証を行いたい機器の他に別途鍵管理装置を必要としている。

【0011】

また、鍵管理装置のような第三者機関を使用せずに二者間だけでDiffie-Hellman法を利用して秘密裏に共通鍵を共有する方式もあるが、Diffie-Hellman法は長い計算時間を必要とし、その間のCPU演算時間を浪費する。そのうえに、Diffie-Hellman法自体は認証は行なわないので、自分の予期しない相手と共通鍵を交換している可能性があり、認証方法としては不完全である。

【0012】

しかし、共通鍵を用いた認証方式は、安全かつ演算負荷をかけずにあらかじめ共通鍵を共有できれば、公開鍵暗号方式を用いた認証方式よりも効率的な認証方式である。

【0013】

本発明は、前記従来の課題を解決するものであり、ネットワークに接続する機器の認証システムにおいて、処理能力が低い機器にも有効な共通鍵を用いて、演算処理負荷が低く、簡単でかつ安全な認証方法を提供することを目的とする。

【課題を解決するための手段】**【0014】**

前記従来の課題を解決するために、本発明の認証方法は、第1の機器とネットワークを介して接続された第2の機器と、前記第1の機器と前記第2の機器が認証のために用いる秘密情報を生成する秘密情報生成装置を備えたシステムにおいて、前記第1の機器と前記第2の機器間の認証の関係を初期設定する際に、前記秘密情報生成装置にて前記秘密情報を生成し、生成した前記秘密情報を前記秘密情報生成装置内に記憶し、前記第1の機器と前記第2の機器に前記秘密情報生成装置内に記憶された前記秘密情報をネットワークを介さずに設定し、前記第1の機器が、前記第2の機器は通信相手として正当であるかを認証する際には前記第1の機器は、前記第2の機器に設定されている前記秘密情報と前記第1の機器に設定されている前記秘密情報の少なくとも一部が一致することを前記ネットワークを介して確認することを特徴とする。

【0015】

本構成によって、演算処理負荷が低く、簡単でかつ安全に機器の認証を行なうことができる。

【発明の効果】**【0016】**

本発明によれば、認証に際し、認証を行う機器同士以外に別途秘密情報を管理する機器を必要とせず、システムの構成が簡単である。

【0017】

また、ネットワークを介さずにユーザが機器に直接秘密情報を設定することで、漏洩することなく秘密情報を設定することができ、かつユーザが認証関係を樹立することを要求する機器同士のみに秘密情報を設定でき、なりすましや不正機器への接続を防止することができる。

【0018】

さらに、秘密情報生成装置において秘密情報を生成することで、ネットワークを介して秘密情報設定のためにDiffie-Hellman法のような演算量の多い処理を必要とせず、各機器のCPU処理負荷が少ない。

【0019】

以上のように、処理能力はできる限り低く抑えることが必要な、たとえばネット家電のような機器においても有効な、演算処理負荷が低く、簡単でかつ安全な認証方法を提供できる。

【発明を実施するための最良の形態】

【0020】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【0021】

(実施の形態1)

図1は、本発明の実施の形態1に係る認証方法が適用されるシステムの構成を示すブロック図である。HGW(ホーム・ゲートウェイ)とNWカメラ(ネットワークカメラ)に本発明を適用した例である。本実施の形態では、認証方式としてチャレンジ・レスポンス方式を用いた認証について説明する。

【0022】

図1において、104はホームネットワーク、101はホームネットワークに接続するHGW、102はホームネットワークに接続するNWカメラ、103は秘密情報生成装置、105、106はHGW101およびNWカメラ102と、秘密情報生成装置103を接続するインタフェースである。なお、インタフェースは、USB、IrDA、赤外線など、接触/非接触を問わず、いずれのインタフェース手段でも構わない。本発明においては限定しない。

【0023】

図2は、本発明の実施の形態1における秘密情報生成装置103の詳細な構成を示すブロック図である。

【0024】

図2において秘密情報生成装置103は、HGW101およびNWカメラ102と秘密情報生成装置103との間で秘密情報の受け渡しを行うインタフェース106と、秘密情報を生成する秘密情報発生部201と、生成した秘密情報を記憶しておく記憶部202と、操作者が秘密情報の生成指示を入力する生成開始ボタン203と、操作者が秘密情報の消去指示を入力する初期化ボタン204と、現在のステータス(秘密情報なし/秘密情報あり)を文字で表示する液晶の表示部206と、上記各部および各装置を制御する制御部205と、を備えている。

【0025】

図3は本発明の実施の形態1における秘密情報生成装置103の処理フローである。

【0026】

制御部205は生成開始ボタン203の押下を検出すると(ST10)、秘密情報発生部201に秘密情報を生成するよう命令信号を送信する。秘密情報発生部201は制御部205からの秘密情報の生成の命令信号を受信すると少なくともHGW101とNWカメラ102が認証のために用いる秘密情報を生成する(ST11)。また、制御部205は生成された秘密情報を記憶するよう記憶部202に命令信号を送信する。記憶部202は制御部205からの秘密情報の記憶の命令信号を受信すると秘密情報発生部201で生成された秘密情報を記憶部202内に記憶し、転送回数をリセットする(ST12)。また記憶部202は秘密情報記憶完了の信号を制御部205に送信し、制御部205は記憶部202からの秘密情報記憶完了の信号を受信すると、表示部206に秘密情報が生成されたことを示すために表示の命令信号を送信する。表示部206は制御部205からの表示の命令信号を受信すると、文字表示を秘密情報ありに変更する(ST13)。

【0027】

制御部205は初期化ボタン204の押下を検出すると(ST14)、秘密情報を消去するよう記憶部202に命令信号を送信し、記憶部202は制御部205からの秘密情報の消去の命令信号を受信すると、記憶部202内に記憶されている秘密情報を消去し、転送回数をリセットする(ST18)。また記憶部202は秘密情報消去完了の信号を制御

部205に送信し、制御部205は記憶部202からの秘密情報消去完了の信号を受信すると、表示部206に秘密情報が消去されたことを示すために表示の命令信号を送信する。表示部206は制御部205からの表示の命令信号を受信すると、文字表示を秘密情報なしに変更する(ST19)。

【0028】

制御部205は、秘密情報が記憶部202に記憶されている状態で、インタフェース106にHGW101またはNWカメラ102のインタフェース105が接続されたことを検出すると(ST15)、秘密情報をHGW101またはNWカメラ102にインタフェース106を介して転送するよう命令信号を送信する。記憶部202は制御部205からの秘密情報の転送の命令信号を受信すると、インタフェース106を介して、HGW101またはNWカメラ102に秘密情報を転送し、転送回数をカウントアップする(ST16)。このとき、転送回数が規定回数になった時点で(ST17)、制御部205に転送終了信号を送信する。なお、本実施の形態では、秘密情報を設定する機器は2台であるため、規定回数は2回としている。制御部205は転送終了信号を受信すると、秘密情報を消去するよう記憶部202に命令信号を送信し、記憶部202は制御部205からの秘密情報の消去の命令信号を受信すると、記憶部202内に記憶されている秘密情報を消去し、転送回数をリセットする。(ST18)。また記憶部202は秘密情報消去完了の信号を制御部205に送信し、制御部205は記憶部202からの秘密情報消去完了の信号を受信すると、表示部206に秘密情報が消去されたことを示すために表示の命令信号を送信する。表示部206は制御部205からの表示の命令信号を受信すると、文字表示を秘密情報なしに変更する(ST19)。

【0029】

図4は、実施の形態1におけるHGW101およびNWカメラ102が有する主要部の詳細な構成を示すブロック図である。HGW101は、秘密情報生成装置103と秘密情報の受け渡しを行うインタフェース105を有し、またNWカメラ102とメッセージの送受信を行うために通信部301を介してネットワーク104に接続される。さらに、秘密情報を記憶する記憶部302と、擬似乱数を生成する乱数生成部303と、擬似乱数と秘密情報から認証情報を生成する認証情報生成部304と、NWカメラ102から受信したメッセージの認証情報と比較して認証情報生成部304で生成した認証情報が一致することを確認する検証部305と、操作者が秘密情報の消去指示を入力する初期化ボタン306と、現在のステータス(秘密情報なし/秘密情報あり/認証済み/認証失敗)を文字で表示する液晶の表示部307と、上記各部を制御する制御部308とを備えている。NWカメラ102も主要部に関してHGW101と同様の構成を有する。

【0030】

図5は実施の形態1におけるHGW101の秘密情報設定時の処理フローである。制御部308は、インタフェース105に秘密情報生成装置103のインタフェース106が接続されたことを検出すると(ST20)、秘密情報を秘密情報生成装置103からインタフェース105を介して取り込むよう命令信号を送信する。インタフェース105は制御部308からの秘密情報の転送の命令信号を受信すると、インタフェース105を介して、秘密情報生成装置103の秘密情報を取り込む(ST21)。また、制御部308は取り込んだ秘密情報を記憶するよう記憶部302に命令信号を送信する。記憶部302は制御部308からの秘密情報の記憶の命令信号を受信すると、受信した秘密情報を記憶部302に記憶する(ST22)。記憶部302は秘密情報記憶完了の信号を制御部308に送信し、制御部308は記憶部302からの秘密情報記憶完了の信号を受信すると、表示部307に秘密情報が設定されたことを示すために表示の命令信号を送信する。表示部307は制御部308からの表示の命令信号を受信すると、文字表示を秘密情報ありに変更する(ST23)。

【0031】

NWカメラ102のインタフェース105に秘密情報生成装置103を接続した場合にも、上記と同様の処理フローにより秘密情報を設定する。

【0032】

図6は本発明の実施の形態1におけるHGW101の認証時の処理フローである。また、図11はHGW101がNWカメラ102を認証する際のメッセージのやり取りを示すものである。なお、認証を開始するタイミングは、操作者が認証開始ボタンを押下することにより認証開始の指示が与えられたとき、または、何らかのアプリケーション等が起動されて認証開始の指示が与えられたとき、もしくは、秘密情報を設定した直後から認証を開始する等、様々考えられるが、本発明においては重要な項目ではなく、認証を開始するタイミングは特定しない。

【0033】

HGW101の制御部308は、認証開始の指示を検出すると（図6：ST30、図11：ST64）、制御部308は乱数生成部303に擬似乱数を生成するよう乱数の生成の命令信号を送信する。乱数生成部303は制御部308からの乱数の生成の命令信号を受信すると、擬似乱数（チャレンジコード）を生成し（図6：ST31、図11：ST65）、乱数生成終了の信号を制御部308に送信する。制御部308は乱数生成終了の信号を受信すると、生成した擬似乱数をNWカメラ102に送信するよう通信部301に送信の命令信号を送信する。また同時に、記憶部302に擬似乱数を記憶するよう乱数の記憶の命令信号を送信する。通信部301は制御部308からの送信の命令信号を受信するとネットワーク104を介してNWカメラ102に擬似乱数を含む乱数メッセージを送信する（図6：ST32、図11：ST66）。記憶部302は制御部308からの乱数の記憶の命令信号を受信すると、生成した擬似乱数を前記秘密情報とは別に記憶部302内に記憶する（図6：ST33）。

【0034】

ここで、制御部308はネットワーク104を介してのNWカメラ102からの認証情報メッセージの受信を待つ。なお、NWカメラ102の動作については後述する。HGW101の通信部301はNWカメラ102から認証情報を含む認証情報メッセージを受信したことを検出すると（図6：ST34、図11：ST6A）、認証情報メッセージから認証情報N（レスポンスコード）を取り出し、制御部308に認証情報メッセージ受信通知の信号を送信する。制御部308は認証情報メッセージ受信通知の信号を受信すると、認証情報生成部304に記憶部302が記憶している擬似乱数と秘密情報とを用いて認証情報を生成するよう命令信号を送信する。認証情報生成部304は制御部308からの認証情報の生成の命令信号を受信すると、記憶部302が記憶している擬似乱数と秘密情報を用いて認証情報Hを生成し（図6：ST35、図11：ST6B）、認証情報生成終了の信号を制御部308に送信する。なお、認証情報の生成はNWカメラ102と同様の手段で行う。制御部308は認証情報生成終了の信号を受信すると、検証部305に認証情報の検証の命令信号を送信する。検証部305は制御部308からの認証情報の検証の生成命令信号を受信すると、認証情報Hと認証情報Nが同値であるかどうか検証する（図6：ST36、図11：ST6C）。検証した結果、認証情報が一致していたら（図6：ST37）、検証部305は認証情報一致の信号を制御部308に送信する。制御部308は認証情報一致の信号を受信すると、表示部307に認証が成功したことを示す表示の命令信号を送信する。表示部307は制御部308からの表示の命令信号を受信すると、文字表示を秘密情報ありから認証済みに変更する（図6：ST38）。

【0035】

以上説明したように、HGW101とNWカメラ102が生成した認証情報が同一であることで、同じ秘密情報を所有していることがわかり、HGW101がNWカメラ102と接続することが正当であることを認証できる。

【0036】

また、検証した結果、認証情報が一致していなかったら（図6：ST37）、検証部305は認証情報不一致の信号を制御部308に送信する。制御部308は認証情報不一致の信号を受信すると、表示部307に認証が失敗したことを示すために表示の命令信号を送信する。表示部307は制御部308からの表示の命令信号を受信すると、文字表示を

秘密情報ありから認証失敗に変更する（図6：ST39）。

【0037】

図7は、実施の形態1におけるHGW101の初期化時の処理フローである。制御部308はHGW101の初期化ボタン306押下を検出すると（ST40）、記憶部302に秘密情報を消去するよう命令信号を送信する。記憶部302は制御部308からの秘密情報の消去の命令信号を受信すると、秘密情報を記憶しているかどうか確認する（ST41）。秘密情報が記憶されていれば消去する（ST42）。記憶部302は秘密情報消去完了の信号を制御部308に送信し、制御部308は記憶部302からの秘密情報消去完了の信号を受信すると、表示部に秘密情報が消去されたことを示すために表示の命令信号を送信する。表示部307は制御部308からの表示の命令信号を受信すると、文字表示を秘密情報ありから秘密情報なしに変更する（ST43）。

【0038】

図8は、本発明の実施の形態1におけるNWカメラ102の認証時の処理フローである。図11はHGW101がNWカメラ102を認証する際のメッセージのやり取りを示すものである。

【0039】

NWカメラ102の通信部301はHGW101から擬似乱数を含む乱数メッセージを受信したことを検出すると（図8：ST50、図11：ST67）、乱数メッセージから擬似乱数（チャレンジコード）を取り出し、制御部308に乱数メッセージ受信の信号を送信する。制御部308は乱数メッセージ受信の信号を受信すると、認証情報生成部304に認証情報を生成するよう命令信号を送信する。認証情報生成部304は制御部308からの認証情報の生成の命令信号を受信すると、擬似乱数と記憶部302が記憶している秘密情報を用いて認証情報N（レスポンスコード）を生成し（図8：ST51、図11：ST68）、認証情報生成終了の信号を制御部308に送信する。制御部308は認証情報生成終了の信号を受信すると、生成した認証情報NをHGW101に送信するよう通信部301に送信の命令信号を送信する。通信部301は制御部308からの送信の命令信号を受信するとネットワーク104上に認証情報Nを含む認証情報メッセージを送信する（図11：ST69）。

【0040】

このように、本実施形態での認証方法では、認証に際し、認証を行う機器同士と秘密情報生成装置以外に別途認証機関や鍵管理機構など特別な機器を必要とせず、システムの構成が簡単である。

【0041】

また、秘密情報を秘密情報生成装置で生成するため、機器（ここではHGW101とNWカメラ102）のCPUの処理負荷が少ない。

【0042】

また、秘密情報生成開始から機器に秘密情報を設定するまでの間は、秘密情報生成装置は操作者が保持しており、この期間に秘密情報が漏洩することはない。また、秘密情報は2台の機器に設定後自動的に秘密情報生成装置から消去されるので、秘密情報生成装置を盗まれても別の場所で秘密情報を不正に使用されることを防止でき、かつ漏洩することはない。

【0043】

なお、本実施の形態ではネットワーク104は有線のホームネットワークとして説明しているが、無線のホームネットワークであってもよい。またホームネットワークに限定されず、一般のネットワーク（有線、無線に係らず）で用いても良い。

【0044】

また、秘密情報生成装置103とHGW101およびNWカメラ102インタフェースの接触の検出法としては、電気的な検出方法、機械的な検出方法等考えられるが、検出方法については特定しない。

【0045】

また、本実施の形態では、表示部 206 は文字を液晶に表示する、として説明したが、文字やマークで表示して知らせる液晶の他、色別で点灯して知らせる LED のような他の視覚的に知らせる方法や、音声や音など聴覚的に知らせる方法、振動など触覚的に知らせる方法等でもよい。本発明においては、表示部 206 について、その手段をおよび形態を特定しない。

【0046】

また、本実施の形態では秘密情報生成装置 103 は記憶している秘密情報を HGW101 および NWカメラ 102 に転送するとして説明したが、HGW101 および NWカメラ 102 が自ら読み取るものでもよい。

【0047】

また、本実施の形態では、秘密情報を転送する際の規定回数を 2 回として説明したが、秘密情報を複数の機器に設定する場合は、秘密情報を設定したい機器の台数を規定回数に設定すればよい。規定回数の設定方法は、本発明においては重要項目でなく、特定しない。

【0048】

また、表示部 307 は、文字を液晶に表示する、として説明したが、現在の状態を文字やマークを表示して知らせる液晶や色別で点灯して知らせる LED 等でもよい。本発明においては重要な項目ではなく、表示手段については特定しない。

【0049】

また、擬似乱数生成に際し、乱数生成手段に何を用いるかは本発明においては特定しない。

【0050】

また、認証情報 H および認証情報 N の生成は、ハッシュ関数による演算が一般的に利用されているが、本発明においては特定しない。

【0051】

また、秘密情報の全てを認証の確認のために用いる必要はない。秘密情報を認証以外に使用しても構わない。

【0052】

また、本実施の形態では、秘密情報を生成するためのボタンと秘密情報を消去するためのボタンを別々のボタンとして説明したが、生成と消去の指示を同じボタンで行うとし、操作者がボタンを押下と同時に秘密情報を生成、記憶し、操作者がボタンの押下をやめたときに秘密情報が消去されるとしてもよい。これにより、同じボタンの操作により生成と消去をする場合は、ボタンを押下している間のみしか秘密情報が保持されないのので、秘密情報生成装置が盗まれて、別の場所で秘密情報が不正使用されることを防止できる。

【0053】

また、本実施の形態では、認証失敗を表示手段で操作者に知らせ、操作者が初期化ボタンを使用して両機器の秘密情報を消去する説明をしたが、認証失敗時に自動的に秘密情報を消去してもよい。

【0054】

また、本実施の形態では、HGW101 と NWカメラ 102 が同一の秘密情報を保持していることを確認するための手段としてチャレンジ・アンド・レスポンス方式を用いて説明したが、共通鍵暗号アルゴリズムやハッシュ関数を用いた他の認証手法でもよい。また、HGW101 が NWカメラ 102 を認証する片側認証として説明しているが、同様の手順で NWカメラ 102 が HGW101 を認証することも可能である（相互認証）。また、その際どちらの機器から認証を行うかの順番は規定せず、同時に行っても構わない。また、本認証方法は、ネット家電機器に限らず、さまざまな機器間の認証で応用可能である。

【0055】

なお、秘密情報生成装置 103 は、持ち運び可能でコンパクトな例えばカード型デバイスなどが適している。

【0056】

なお、本発明はIPsecを用いた暗号通信を行うため装置に対する事前共通鍵の設定にも有用であることは当事業者であれば自明である。

【産業上の利用可能性】

【0057】

本発明にかかる認証方法では、演算処理負荷が低く設定が簡単になるという効果が得られるので、例えば、ネット家電機器を接続するホームネットワークシステムにおける認証方法等として有用である。また、ネット家電機器に限らず、機器間の認証を必要とするネットワークシステム等においても適用できる。

【図面の簡単な説明】

【0058】

【図1】本発明の実施の形態1における認証方法が適用されるシステムの構成を示す図

【図2】本発明の実施の形態1における秘密情報生成装置103の詳細な構成を示すブロック図

【図3】本発明の実施の形態1における秘密情報生成装置103の処理フローを示す図

【図4】本発明の実施の形態1におけるHGW101およびNWカメラ102の詳細な構成を示すブロック図

【図5】本発明の実施の形態1におけるHGW101の秘密鍵設定時の処理フローを示す図

【図6】本発明の実施の形態1におけるHGW101の認証時処理フローを示す図

【図7】本発明の実施の形態1におけるHGW101の初期化時の処理フローを示す図

【図8】本発明の実施の形態1におけるNWカメラ102の認証時処理フローを示す図

【図9】特許文献1を説明するための図

【図10】特許文献2を説明するための図

【図11】HGW101とNWカメラ102のメッセージのやり取りを示す図

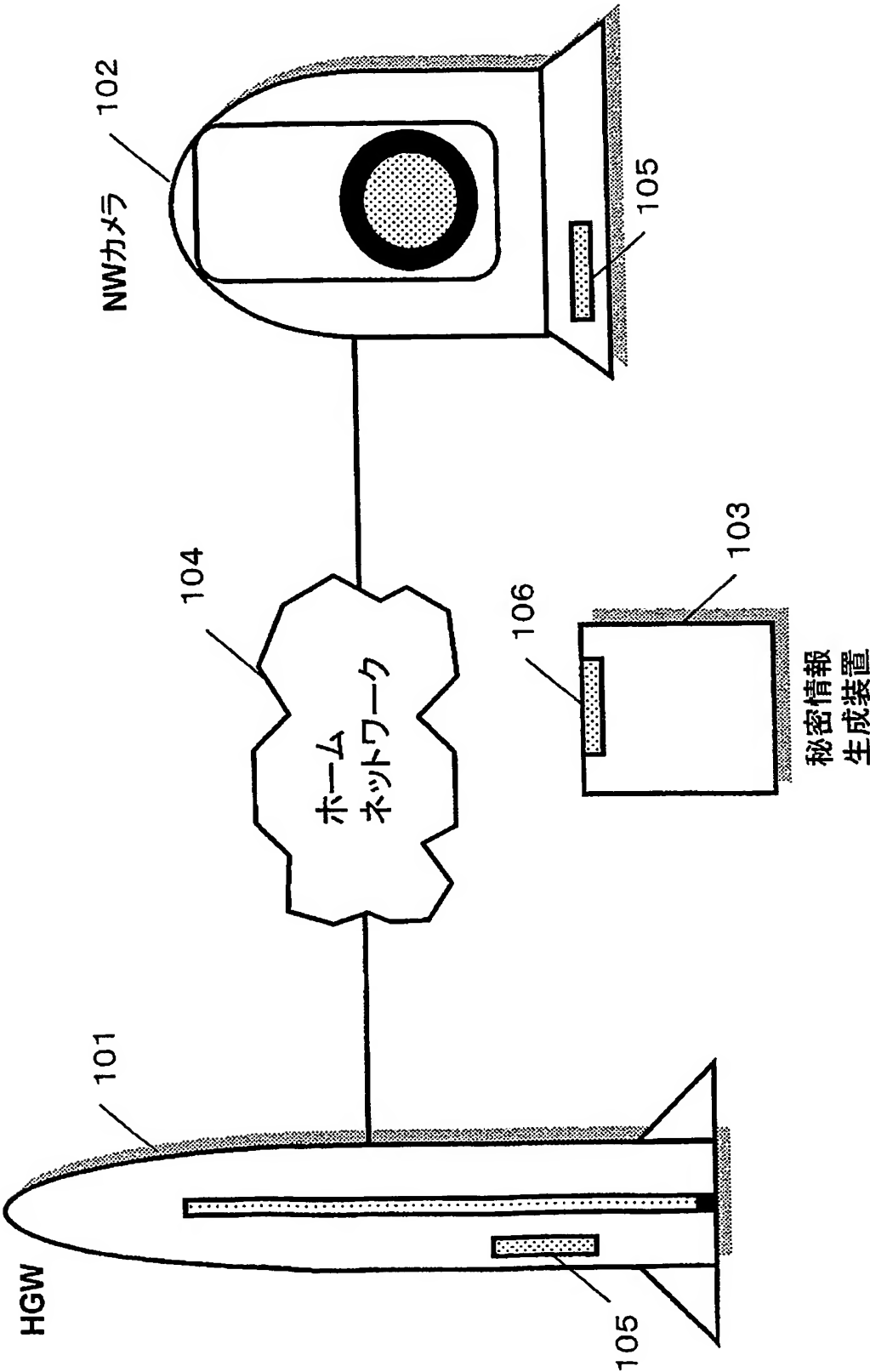
【符号の説明】

【0059】

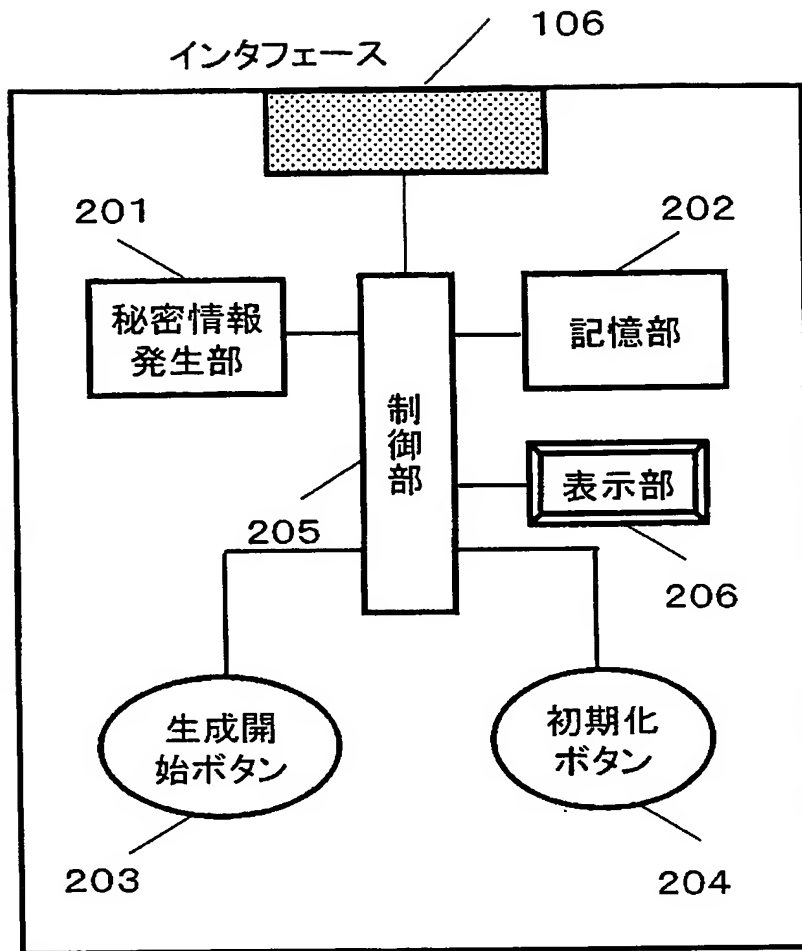
- 101 HGW
- 102 NWカメラ
- 103 秘密情報生成装置
- 104 ホームネットワーク
- 105, 106 インタフェース
- 201 秘密情報発生部
- 202, 302 記憶部
- 203 生成開始ボタン
- 205, 308 制御部
- 204, 306 初期化ボタン
- 301 通信部
- 303 乱数生成部
- 304 認証情報生成部
- 305 検証部
- 206, 307 表示部

【書類名】 図面
【図 1】

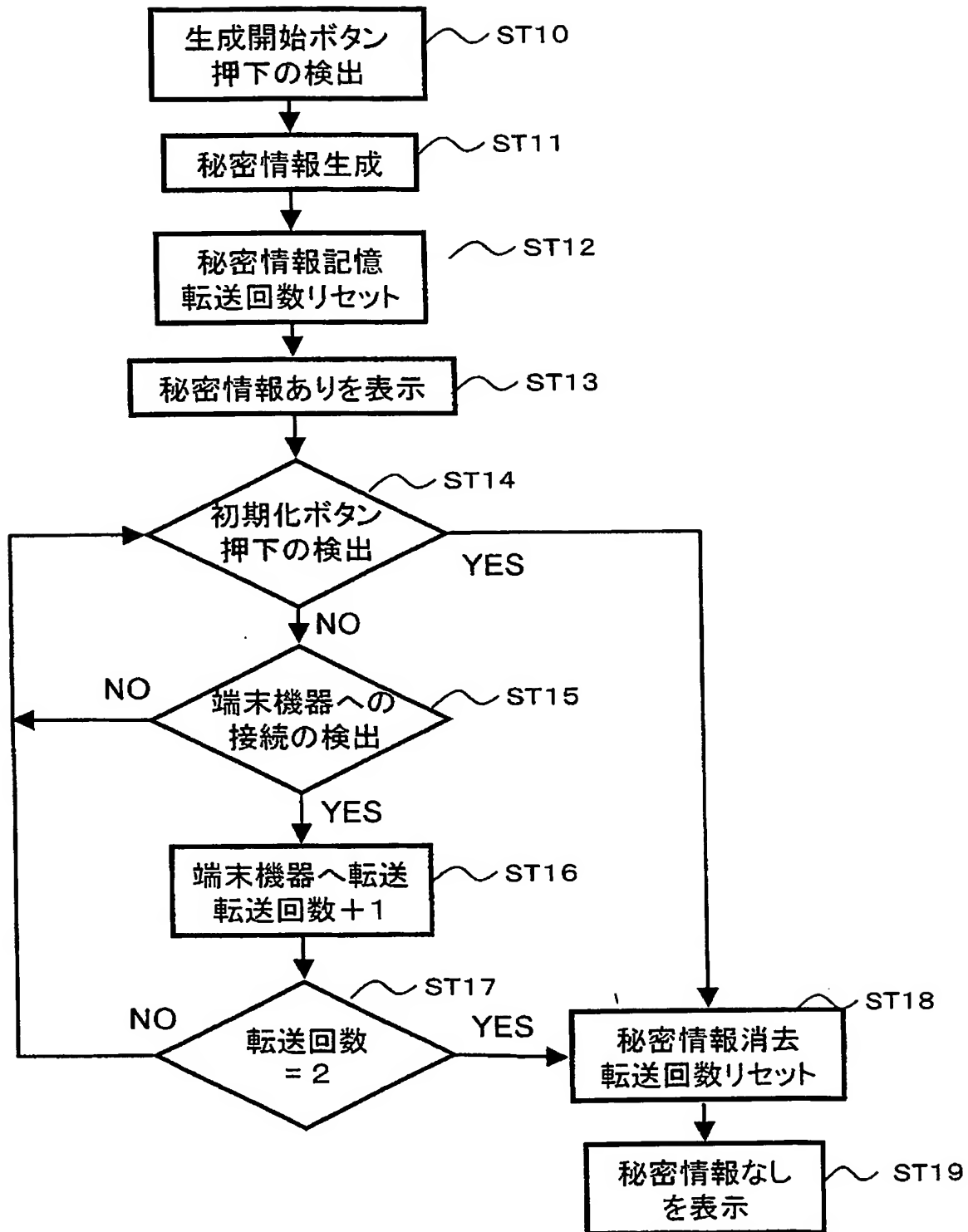
ネット家電機器の認証システム



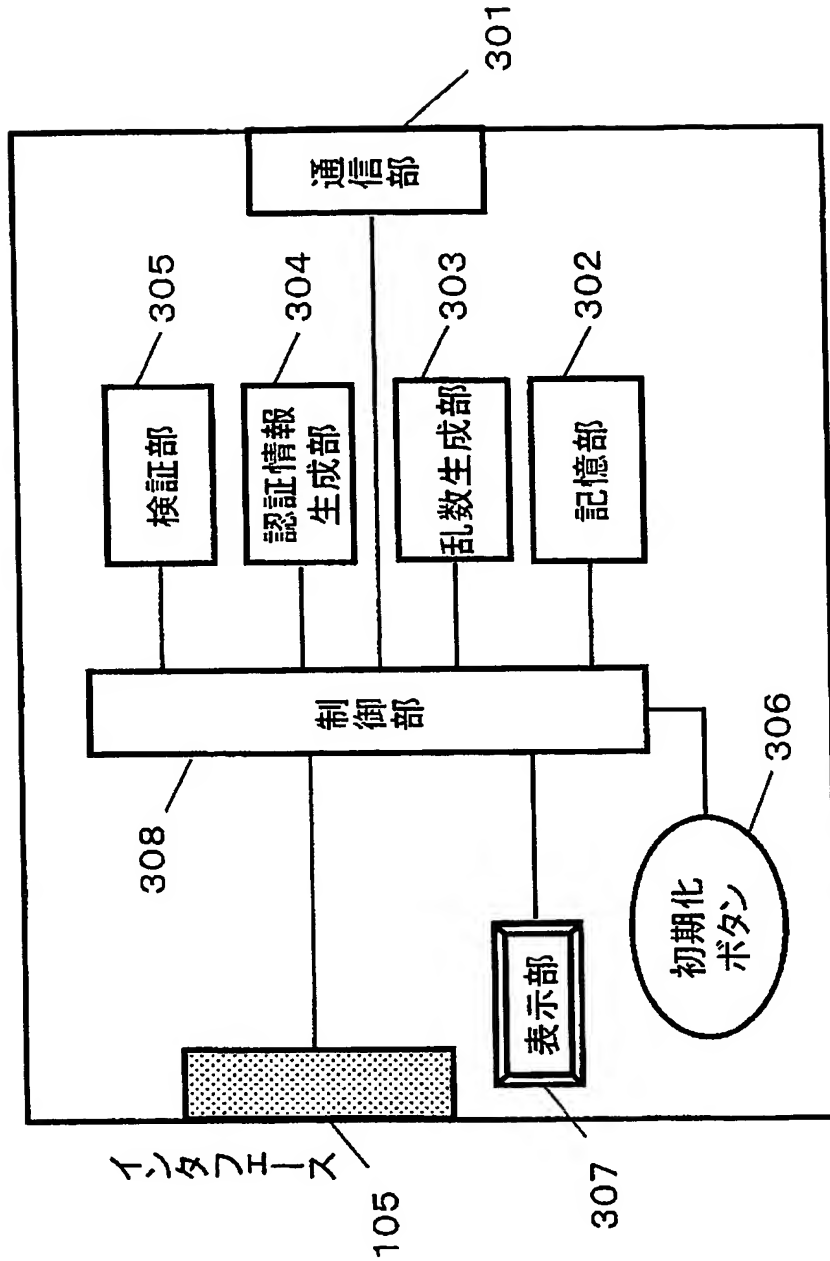
【図 2】



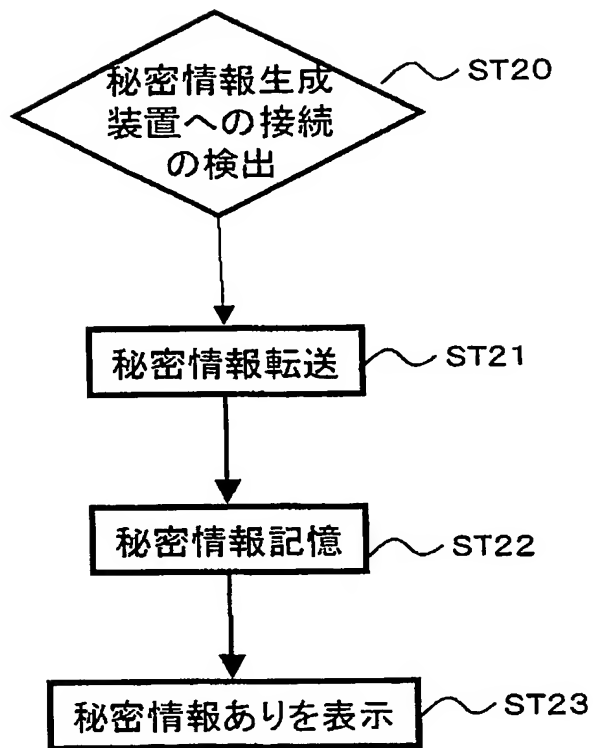
【図 3】



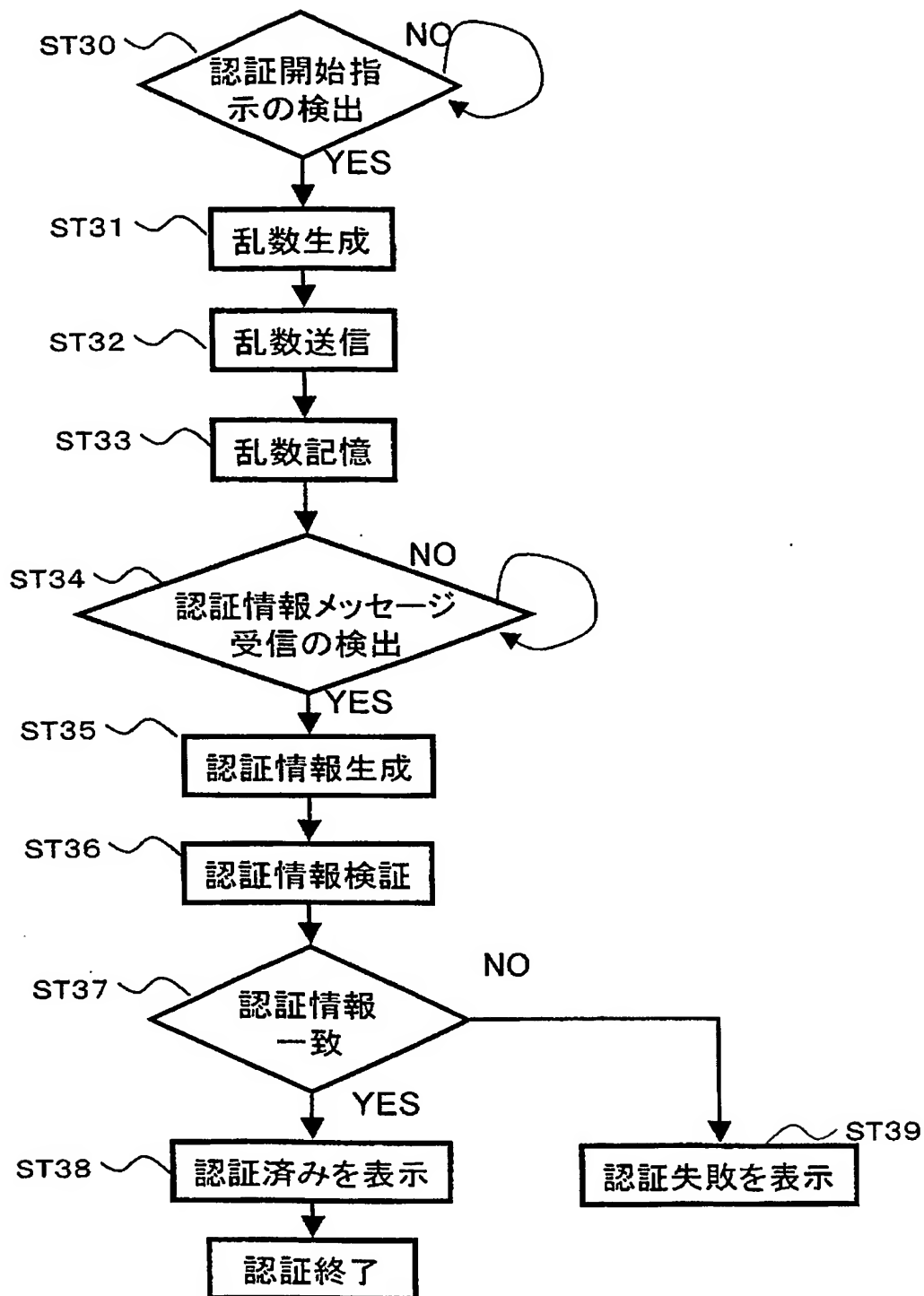
【図 4】



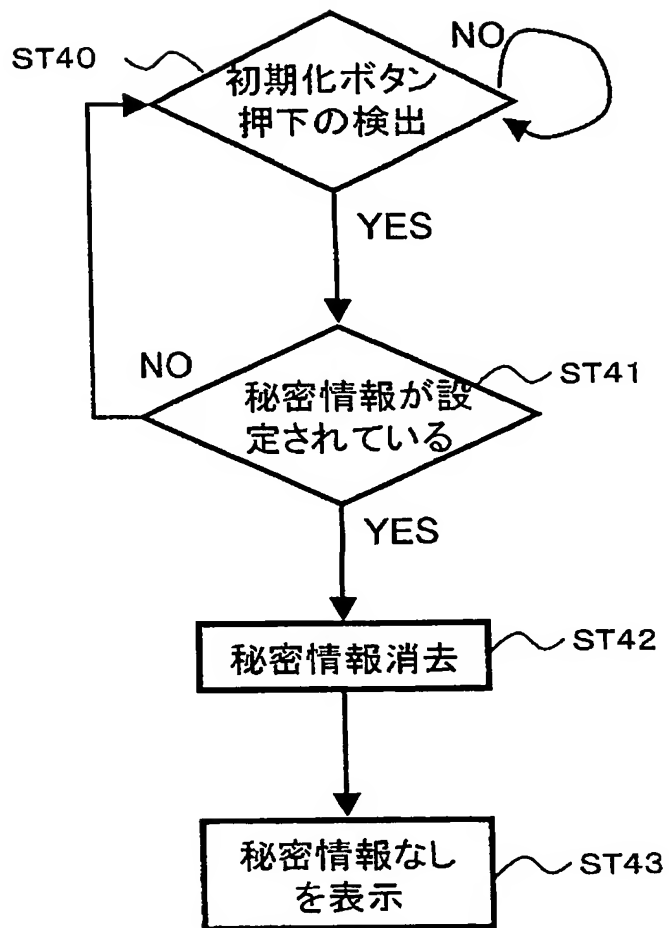
【図 5】



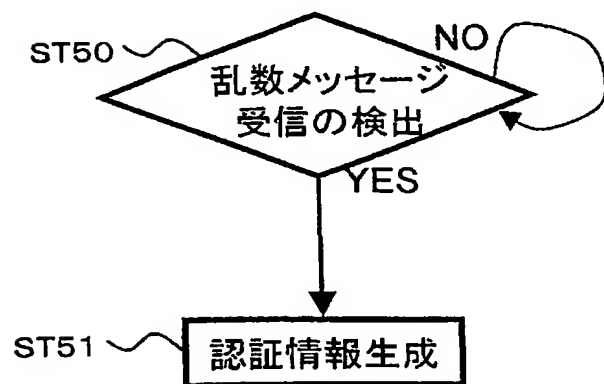
【図6】



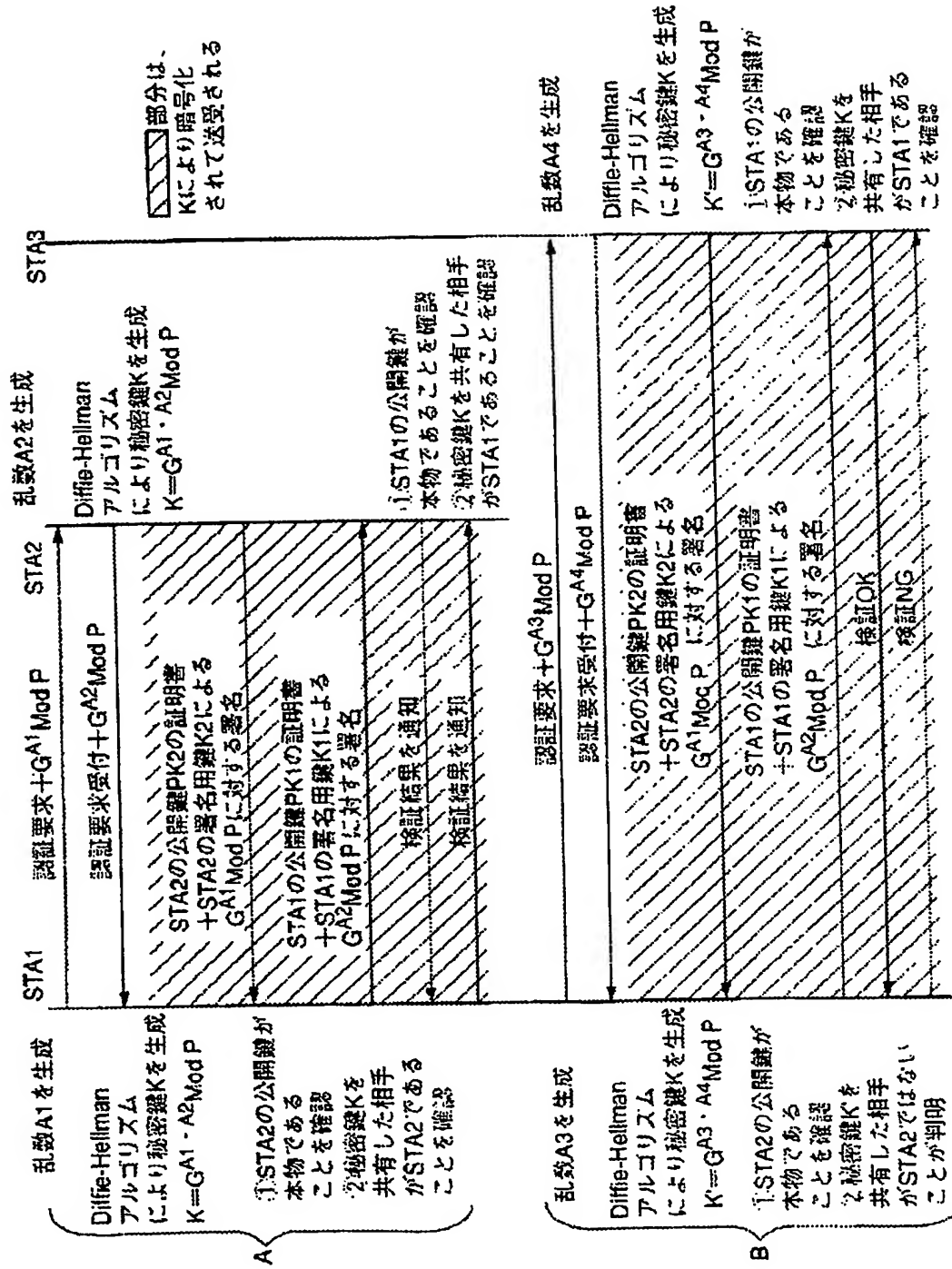
【図 7】



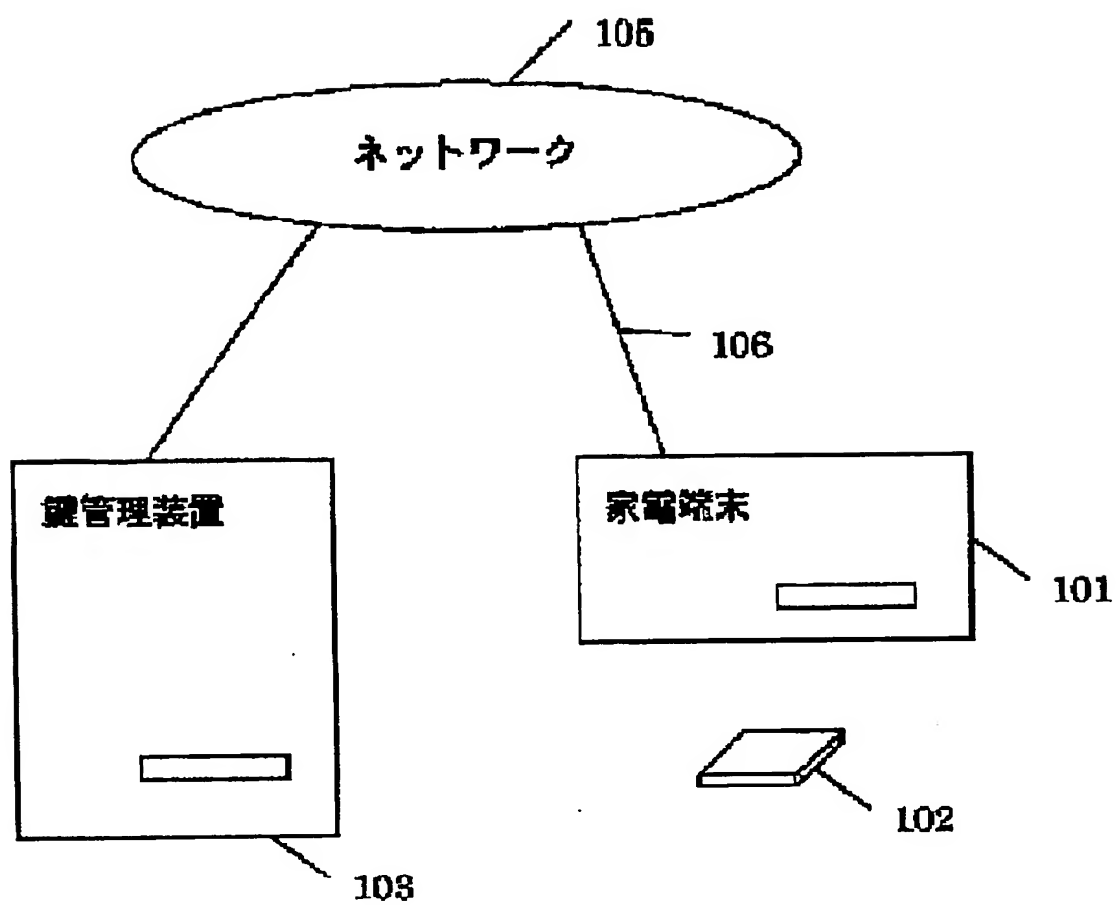
【図 8】



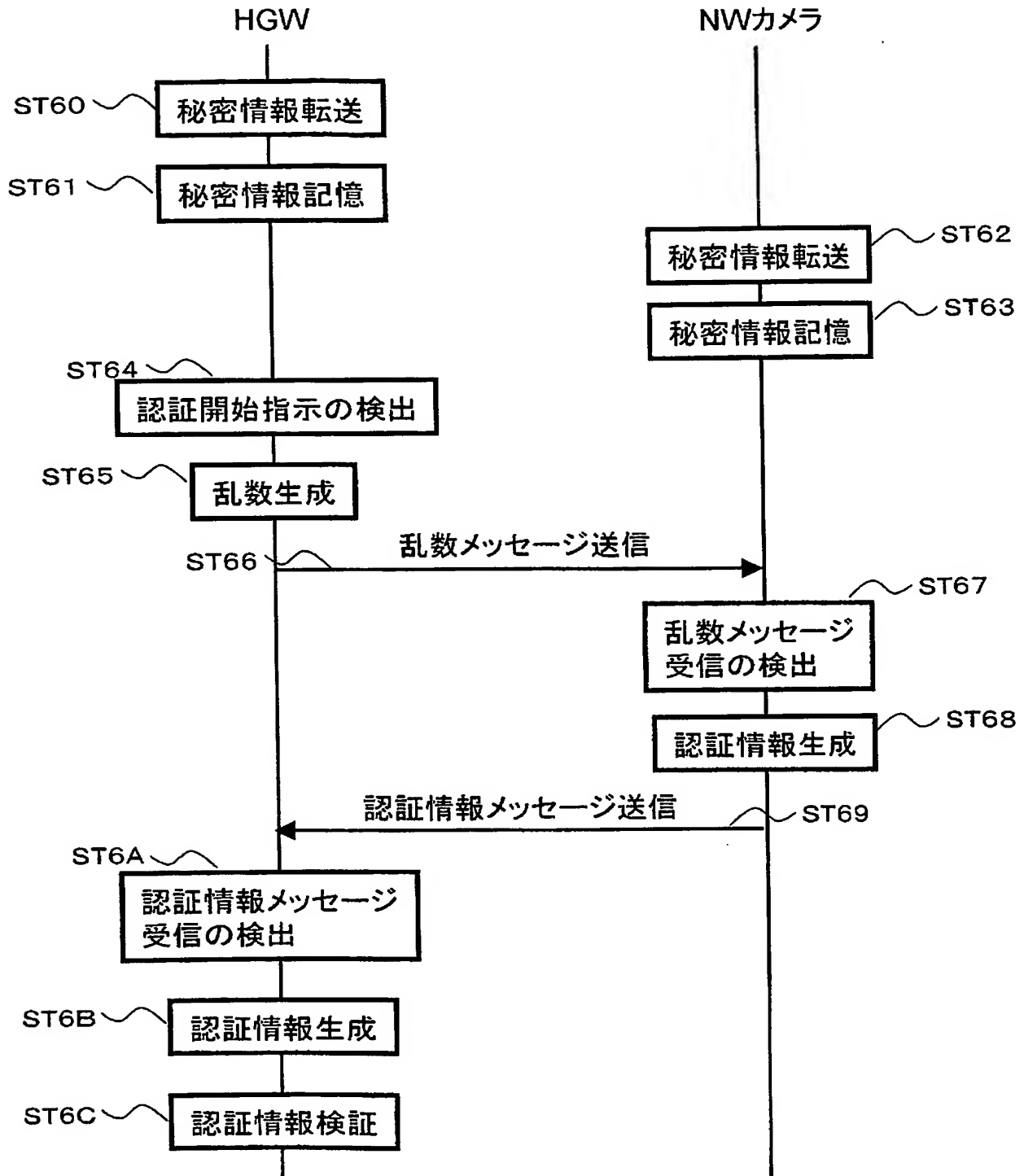
【図9】



【図 10】



【図11】



【書類名】要約書

【要約】

【課題】機器に大きな処理能力や計算時間を必要とする従来の公開鍵暗号方式を利用する認証方法などは、ネット家電機器のようなCPUやメモリ等リソースが乏しい機器には不向きである。ネット家電機器を含む通信機器において、演算処理が少なく、簡単でかつ安全な認証方法を提供する。

【解決手段】機器101と機器102は、ネットワーク104を介して接続され、認証のために用いる秘密情報を生成する秘密情報生成装置103を備えたシステムにおいて、秘密情報生成装置103において秘密情報を生成し、インタフェース105を介して両機器に秘密情報設定し、ネットワーク104を介して両機器が保持している秘密情報が同一のものであることを確認することにより、通信相手として正当であることを認証する。

【選択図】図1

特願 2 0 0 3 - 4 1 6 1 8 8

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018988

International filing date: 14 December 2004 (14.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-416188
Filing date: 15 December 2003 (15.12.2003)

Date of receipt at the International Bureau: 04 February 2005 (04.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse